Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, May 22, 2023

U.S. Law Enforcement Disrupts Networks Used to Transfer Fraud Proceeds, Taking Over 4,000 Actions in Fifth Campaign

Over 12,000 Actions Taken Since Campaigns Began

The Justice Department, FBI, U.S. Postal Inspection Service (USPIS), and other federal law enforcement agencies announced today the completion of a three-month campaign that disrupted networks used by foreign fraudsters to obtain fraud proceeds. Multiple law enforcement actions addressed conduct by individuals sometimes referred to as "money mules," who have been providing critical services to fraudsters by receiving money from fraud victims and forwarding the fraud proceeds to the perpetrators (many of whom are based overseas). Some individuals knew they were facilitating fraud, while others first interacted with fraudsters as victims and may have been unaware that their activity furthered criminal activity.

Over approximately the last three months, law enforcement took over 4,000 actions against individuals responsible for facilitating a range of fraud schemes. These schemes included those that targeted consumers, such as lottery fraud and romance scams, as well as those that targeted businesses or pandemic funds.

The thousands of actions taken by law enforcement — which ranged from criminal prosecutions to civil actions, to warning letters — were designed to punish those who knowingly assisted fraudsters and to advise those who may have been unknowingly helping fraudsters that their conduct furthered crime. These actions are intended to deter overseas fraudsters from relying on U.S.-based individuals to facilitate schemes and thereby reduce the harm caused by foreign fraud operations.

This year's effort marked the fifth U.S. law enforcement campaign disrupting these money transmitting networks. Since the first campaign, during which approximately 400 actions were taken by law enforcement, agencies have collectively taken over 12,000 actions. Investigations have shown that disrupting money transmitting networks has impeded fraudsters' abilities to receive funds, thereby reducing fraud victimization. These campaigns are part of a global effort to tackle money transmitting networks linked to illegal activity.

"Law enforcement is committed to reducing fraud using every tool at our disposal. Our efforts to disrupt networks used to transfer fraud proceeds, to educate the public about elder fraud, and to prosecute those involved in these schemes have stymied fraudsters," said Associate Attorney General Vanita Gupta. "This initiative demonstrates what can be achieved through focused efforts and vigorous enforcement."

"The money mule campaign was an effort to educate the public, disrupt criminal enterprises, and provide feedback to financial institutions who go to great lengths to implement anti-money laundering programs," said Assistant Director Luis Quesada of the FBI's Criminal Investigative Division. "The FBI values the partnership of the Justice Department's Consumer Protection Branch, USPIS, and other federal agencies who work together to disrupt criminal enterprises conducting fraud and money laundering schemes."

"Anyone can be approached to be a money mule, but criminals often target students, those looking for work, and those on dating websites," said USPIS Inspector in Charge Eric Shen of the Criminal Investigations Group. "When those individuals use the U.S. Mail to send or receive funds from fraudsters, postal inspectors are quick to step in and put a stop to money mule activities."

This year's effort was coordinated by the Justice Department's Consumer Protection Branch, FBI and USPIS, which were joined by Homeland Security Investigations, the Department of Labor Office of Inspector General and the Small Business Administration Office of Inspector General. Participating agencies collectively served over 4,000 letters warning individuals that their activities are facilitating fraud. These letters outlined the potential consequences for continuing to transmit illegally acquired funds. Participating agencies also filed 12 civil or administrative actions. Additionally, more than 25 individuals were criminally charged for knowingly receiving and forwarding victim funds or otherwise laundering fraud proceeds.

- The U.S. Attorney's Office for the District Massachusetts charged a defendant for using his accounting and "virtual CFO" business as a front to launder the proceeds of internet fraud schemes. As part of the alleged conspiracy, the defendant created dozens of shell companies and used those shell companies to open business bank accounts in Rhode Island and Massachusetts, through which the defendant laundered the criminal proceeds for his clients in exchange for fees. In total, since 2019, the defendant is alleged to have opened approximately 80 bank accounts (purportedly on behalf of 65 different companies), laundering approximately $35 million.

- The U.S. Attorney's Office for the Western District of North Carolina charged an individual for facilitating an international, multimillion-dollar tech support fraud. The indictment alleged that the defendant agreed to obtain payment-processing services in his name to process victim payments and laundered the proceeds domestically and internationally to bank accounts located in India, receiving 3% of the revenue in return.

- The U.S. Attorneys' Offices for the Central District of California and the District of Nebraska charged individuals who, despite warnings from law enforcement, continued facilitating fraud. In the Central District of California, an individual was charged for her role in receiving funds from fraud victims, including victims of business email compromises. According to the charges, the defendant opened 11 bank accounts at seven separate financial institutions in furtherance of the scheme. In the District of Nebraska, two individuals were charged for facilitating a lottery fraud scheme, including by receiving cashier's checks in the mail.

As in past years, participating agencies are working to raise awareness about how fraudsters recruit and use individuals to assist their fraud operations. Federal agencies conducted outreach to the public and industry, and also expanded partnerships with local, state, and foreign law enforcement agencies. The Commodities Futures Trading Commission released a public awareness message about how fraudsters use and recruit people to facilitate romance fraud and "wrong number" text message scams, where fraudsters strike up conversations touting their wealth and success in trading crypto assets, over-the-counter foreign currency, or gold contracts to try and convince consumers to "invest" in crypto assets.

The agencies involved in this effort urge consumers to be on the lookout for signs someone is trying to recruit them to receive and transmit fraud proceeds. Do not agree to receive money or checks mailed to you or sent to your bank account for someone you have met over the phone or online. Do not open a bank or cryptocurrency account at someone else's direction. Fraudsters will lie to persuade you to help them. They may falsely tell you that they are helping you get a lottery prize, initiate a purported romantic relationship and then tell you that they need money, or pretend to offer you a job, an opportunity to invest in a business venture, or the chance to help in a charitable effort.

For more information on this initiative, please visit www.justice.gov/civil/consumer-protection-branch/money-mule-initiative.

Information about the Department of Justice's Elder Fraud Initiative is available at www.justice.gov/elderjustice. If you or someone you know is age 60 or older and has been a victim of financial fraud, help is available at the National Elder Fraud Hotline: 1-833-FRAUD-11 (1-833-372-8311).

Information about the Justice Department's COVID-19 Fraud Enforcement Task Force is available at www.justice.gov/coronavirus.

For more information about the Consumer Protection Branch and its enforcement efforts, visit its website at www.justice.gov/civil/consumer-protection-branch.

A criminal indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Topic(s):
Elder Justice
Financial Fraud

Component(s):
Civil Division
Federal Bureau of Investigation (FBI)

Press Release Number:
23-589